2004

# Information System Risks and Risk Factors: Are They Mostly about Information Systems?

Susan A. Sherer

Steven Alter

Communications of the Association for Information Systems

# INFORMATION SYSTEM RISKS AND RISK FACTORS: ARE THEY MOSTLY ABOUT INFORMATION SYSTEMS?

Susan A. Sherer
*College of Business and Economics*
*Lehigh University*
sas6@lehigh.edu

Steven Alter
*School of Business and Management*
*University of San Francisco*

**ABSTRACT**

This article is the second of two whose goal is to advance the discussion of IS risk by addressing limitations of the current IS risk literature. The first article [Alter and Sherer, 2004] presented a general, but broadly adaptable model of system-related risk that addressed the limited usefulness of existing IS risk models for business managers. In this article, we focus on organizing risk factors to make them more useful and meaningful for business managers.

This article shows how the nine elements of the work system framework can be used to organize the hundreds of risk factors in the IS risk literature. It also shows that many of the most important and most commonly cited risk factors for IS in operation and IS projects are actually risk factors for work systems in general. Furthermore, risk factors initially associated with one type of system (e.g. ERP implementation) are often equally relevant at other levels (e.g., information systems projects or work systems in general). Over half of the risk factors in a representative sample of the IS risk literature are valid for work systems in general. This conclusion is a step toward useful risk diagnostic tools based on an organized set of risk factors that are meaningful to business managers and IT professionals.

**Keywords**: risk factors, risk components, work system, information systems risk, project risk, software risk, work system framework, work system life cycle model, implementation

## I. INTRODUCTION

Information systems risk discussions go back at least 30 years. Hundreds of articles identify information system-related success factors or risk factors. Hundreds of risks and risk factors related to information systems and projects have been identified. Regardless of whether any particular article contains 3 or 5 or 35 of them, the lack of an underlying theory or organizing framework limits the managerial usefulness of these lists. Managers would be supported more effectively if they knew:

- how the various factors relate to one another

- why a particular list should be viewed as reasonably complete
- how risk factors can be organized in a meaningful way that helps managers identify and mitigate these risks.

The sheer number of risks and risk factors makes it all the more important to use an organizing framework.

Furthermore, many of the identified risk factors apply to software development projects rather than systems in operation. Although it is certainly legitimate to reflect the concerns of large scale software development organizations attempting to produce software to satisfy requirements, a risk literature that over-emphasizes these concerns inevitably under-emphasizes issues about systems in organizations which are subject to a broad range of risks more related to the work and the environment than to the software itself. This type of imbalance in the literature can lead to gaps in providing guidance for risk management.

After reviewing the nature of the risks and risk factors discussed in the IS literature, this article addresses three main goals:

- demonstrating that the risk factors in the IS risk literature can be categorized using the work system framework
- demonstrating that risk factors initially associated with one type of system (e.g. ERP implementations) are often equally relevant at other levels (e.g. work systems in general).
- demonstrating that the work system framework can be combined with the work system life cycle model to provide an additional level of organization of risk factors.

The overall purpose is to make available knowledge more usable, thereby facilitating risk analysis efforts by business managers. The inheritance-based codification of risk factors that is presented could be applied in diagnostic tools to help managers. Follow-on research will attempt to generate risk diagnostics for managing risk in system development, system implementation, and system operations using the work system framework.

## II. THE NEED TO ORGANIZE INFORMATION SYSTEMS RISKS AND RISK FACTORS

Our attempt to organize information system risks and risk factors was motivated by the results of a survey of the IS risk literature. Attempting to represent the reasonably recent literature rather than covering the hundreds of articles directly or indirectly related to IS risk, our literature survey focused on three journals consistently ranked among the best IS research journals (*MISQ*, *ISR*, and *JMIS)* and selected articles starting in 1986 whose title included the word *risk* or whose abstract focused on risks in system projects or operation. We supplemented this group of articles with other risk-related articles that we believed were significant based on our knowledge of the literature. In total we included 46 articles, and we believe these articles are a good representation of the literature. Appendix I in our companion article [Alter and Sherer, 2004] lists these articles and categorizes them in terms of:

- definition of risk,
- model or approach used,
- type of system or project (which reflects different stages of the software life cycle and some aspects of the temporal nature of risk), and
- number and type of risk variables.

The general conclusion from our literature survey is that the IS risk literature is a jumble of diverse risk models and partially overlapping, atheoretical lists of risk factors and risk components. Our companion article addresses an important shortcoming of the literature, the lack of a practical model that most managers can use for understanding IS-related risks at whatever level of detail is appropriate for them. The current article explores the literature's coverage of risk components and risk factors.

## CONCEPTUALIZATIONS OF RISK

As is explained in our companion article, system-related risk is about risks for work performed during a time interval. This work may be an entire project, a phase in a project (such as development or implementation), or the operation of a work system during the time interval in question. We believe that risk is fundamentally about uncertainty in work performance and the resulting outcomes.

The IS risk literature uses several different conceptualizations of risk. Table 1 summarizes the distribution of risk conceptualizations in the 46 articles selected from the IS risk literature. Most of these conceptualizations focus on negative occurrences and fall into three categories:

- risk components,
- risk factors, and
- probability of negative outcomes.

We believe the prevalence of the negative outcomes conceptualization reflects managerial behavior focusing on reducing the probability of consequences related to missing goals.

Table 1. Conceptualizations of Risk in 46 IS Risk Articles

| ***Conceptualization of risk*** | ***Number of articles*** |
|---|---|
| Risk components: different types of negative outcomes | 11 |
| Risk factors leading to loss or source of risk factors | 11 |
| Risk as probability of negative outcomes (sometimes weighted by loss) | 15 |
| Risk as difficulty in estimating outcome | 2 |
| Risk undefined or discussed using a different term such as problem or threat | 7 |

### Risk as Risk Components or Types of Negative Outcomes

Table 2 illustrates the first category by identifying different types of negative outcomes, such as:

- project risk (projects that cannot be completed within budget, schedule and/or quality constraints),
- functionality risk (projects that fail to deliver functionality),
- political risk (systems that change power relationships with suppliers), or
- security risk (systems that are insecure).

Table 2. Examples of Risk Components in the Literature

| ***Risk components*** | ***Source*** |
|---|---|
| • Financial risk<br>• Security risk<br>• Technology risk<br>• People risk<br>• Information risk<br>• Business process risk<br>• Success risk | [Smith et al. 2001] |
| • Political risk<br>• Financial risk<br>• Technical risk<br>• Functionality risk<br>• Project risk<br>• Systemic risk | [Clemons 1991; Clemons 1995; Clemons et al. 1995] |

| | |
|---|---|
| • Business risk<br>• Systems security risk<br>• Project risk | [Straub and Welke 1998] |
| • Competitive risk<br>• Transition risk<br>• Business partner risk | [Viehland 2002] |
| • Monetary risk<br>• Project risk<br>• Functionality risk<br>• Organizational risk<br>• Competitive risk<br>• Environmental risk<br>• Systemic risk<br>• Technological risk | [Benaroch 2002] |

### Risk as Factors Leading to Loss

Table 3 illustrates the second category by identifying typical risk factors related to information systems. The idea of risk factors is familiar in everyday life; for example, in the way people talk about the risk of heart attack and the risk factors (such as heredity, smoking, stress, and high blood pressure) that tend to increase the risk. Just as success factors[1] are often viewed as factors whose presence increases the probability of success, risk factors are factors whose presence increases the probability of negative outcomes. Risk factors may include individual factors such as size of project, new software, or malicious employees. Some studies combine risk factors from various sources such as task, technology, or actors [Lyytinen et al. 1996]. Others divide these risks into finer categories, focusing for example on factors associated with specific types of actors, e.g. team's lack of expertise or user's lack of expertise [Barki et al. 2001].

Table 3. Examples of Risk Factors in the Literature

| ***Risk factors*** | ***Source*** |
|---|---|
| • Technological newness<br>• Application size<br>• Lack of expertise<br>• Application complexity<br>• Organizational environment | [Barki et al. 2001] |
| • Lack of top management commitment<br>• Failure to gain user commitment<br>• Misunderstanding requirements<br>• Lack of user involvement<br>• Failure to manage end user expectations<br>• Changing scope<br>• Lack of required knowledge<br>• Lack of frozen requirements | [Keil et al. 1998] |

[1] The term success factor is used in a number of different ways. In the implementation literature, a success factor is a factor whose presence increases the probability of success, just as risk factors do the opposite. A different use of the term that was popularized for IS planning in the 1980s is "critical success factor" (CSF), an aspect of a business or a high-level business goal that is critical for business success and therefore should be addressed by the IS plan. For example, Rockart and Crescenzi [1984] say that the CSFs for one company include improving customer and supplier relationships, making the best use of inventory, and using capital and human resources efficiently and effectively.

| | |
|---|---|
| • Introduction of new technology<br>• Insufficient staffing<br>• Conflict between user departments | |
| • Personnel shortfalls<br>• Unrealistic schedules and budgets<br>• Continuous stream of requirements changes<br>• Shortfalls in externally furnished components or tasks | [Boehm 1988; 1989] |
| • Poor concept<br>• Technical infeasibility<br>• Lack of available funding<br>• Lack of market<br>• Telecommunication problems<br>• Vendor problems<br>• Interorganizational problems<br>• Leading edge technology and idea<br>• Competitor copying<br>• Oversubscription<br>• High maintenance cost<br>• Exit barriers<br>• Technology sophistication<br>• Organizational inflexibility | [Kemerer and Sosa 1991] |

**Risk as Probability of Negative Outcomes**

Approximately 1/3 of the studies suggest that risk should be measured as a probability distribution of negative outcomes, often weighted by financial loss. When the IS risk literature deals with probabilities, it tends to show estimates of the probabilities of negative outcomes based on statistical techniques or subjective estimates. Sometimes the negative outcomes are converted to monetary terms and expressed as monetary losses in relation to goals and expectations.

## SITUATIONS STUDIED IN THE INFORMATION SYSTEM RISK LITERATURE

Table 4 shows the range of situations studied in our representative sample of the IS risk literature. Some studies focused primarily on software projects that claim victory when the software is completed and debugged. In contrast, information system projects declare victory when the new or revised information system operates in the organization and is accepted. For that reason, risk studies for information systems projects include more factors related to the project's customer and/or what it produced for the customer. Risk studies focusing on special types of IS projects tended to find risk factors similar to those for IS projects in general. Other studies focusing on IS in operation found some risks such as operational security breaches that are specific to IS operations, but other risks such as inadequate personnel are common to both projects and systems in operation.

Table 4. Focus of Risk Studies in our Literature Survey

| **Focus** | ***Number of Articles*** | |
|---|---|---|
| **IS Projects** | | **38** |
| General IS projects | 19 | |
| Special types of IS projects (ERP, SIS, EIS, reengineering) | 10 | |
| Software projects | 9 | |
| **IS in Operation** | | **12** |
| Special types of systems (IOS, EIS, Healthcare) | 5 | |
| General IS in operation | 7 | |

Note: Four articles discussed both IS projects and IS in operation.

## LIMITATIONS OF THE CURRENT LITERATURE FOR MANAGERS

The literature related to IS risk mentions many risk components (Table 2) and numerous risk factors (Table 3) that could apply in different types of situations (Table 4). An additional problem is that many of the risk components and risk factors overlap, as is illustrated in Figures 1 and 2.

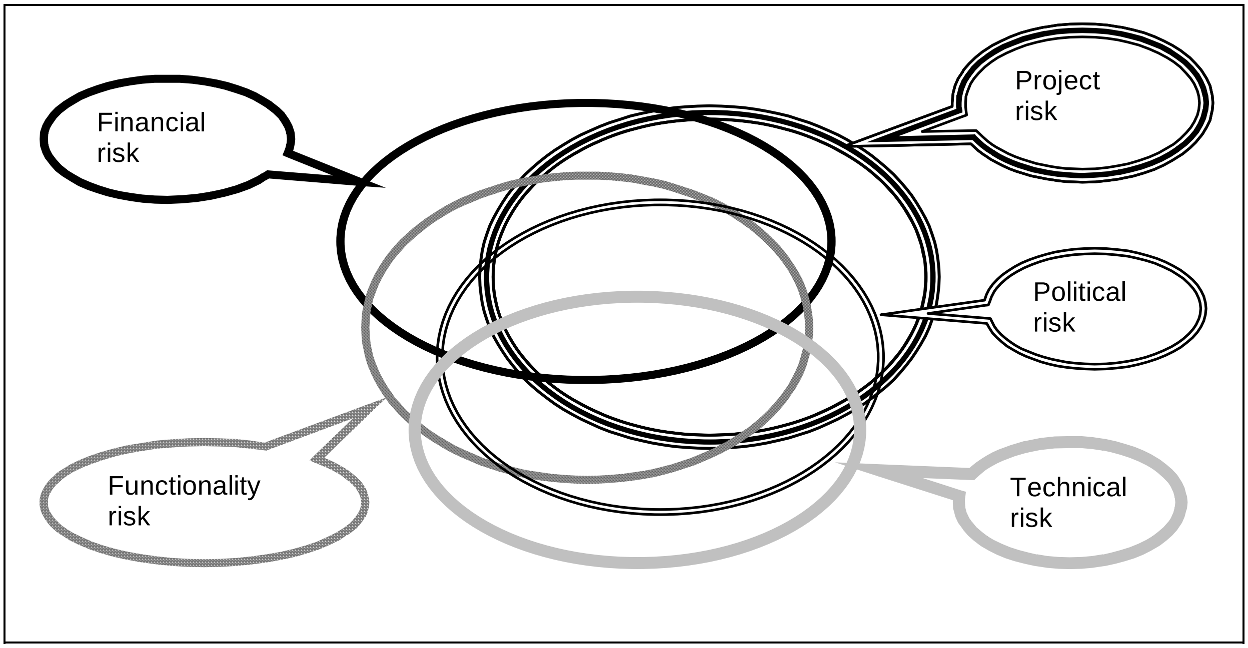



Figure 1: High Degree of Overlap Among Risk Components

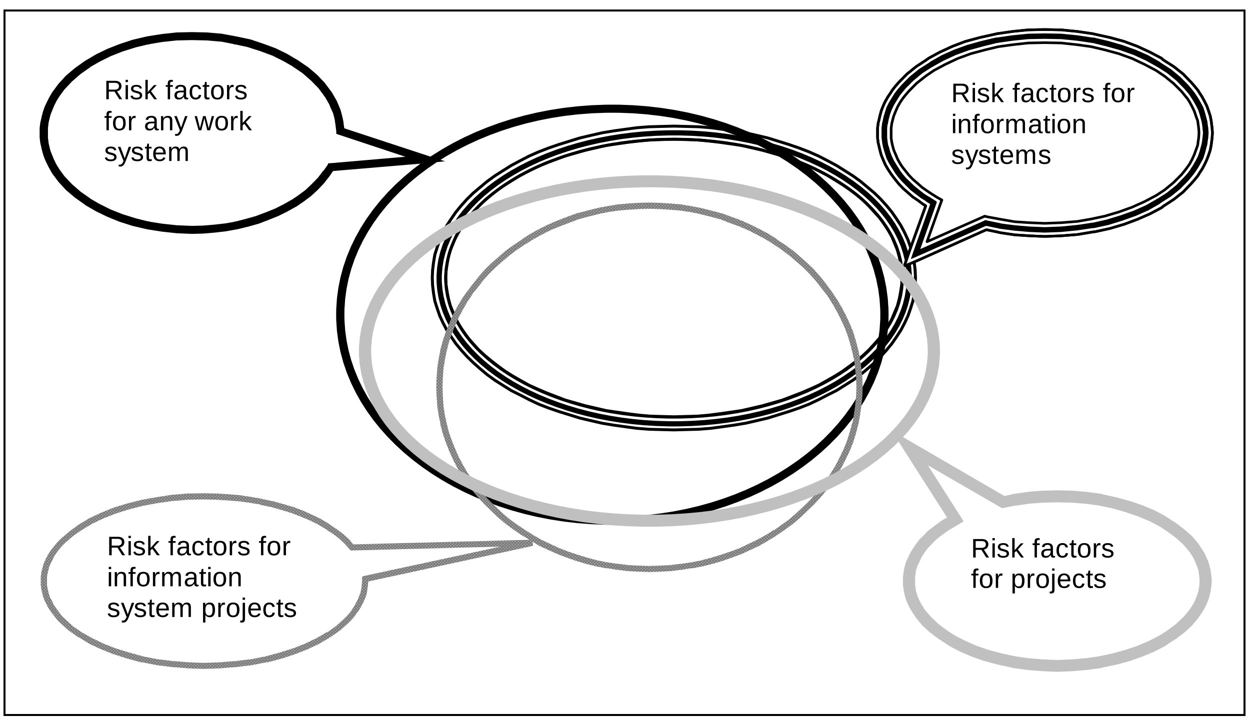



Figure 2: High Degree of Overlap Among Risk Factors for Different Situations

The goal of describing risk components is to help organize risks through categories that cluster things that could go wrong. However, Figure 1 illustrates that typical risk components mentioned in the IS literature overlap substantially and therefore are not independent, as seems to be implied by the term ‘component’. For example, technical risk in a project is part of the overall project risk and contributes directly to both functionality risk and financial risk. Moreover, different articles focus on different clusters of risk components so that the risk manager is uncertain of whether any particular list is complete.

Studies that focus on risk factors often list sets of risk factors without organizing them to increase their usefulness for risk managers. (But some do organize risk factors. For example, Lyytinen [1996] and Lyytinen [1998] categorize risks according to task, structure, actors, technology and interdependencies. Higuera [1996] classifies software risks by class, element, and attribute.)

Risk factors may apply at many different levels. Without reading the articles listed in Table 3, it is not obvious whether many of these are risk factors for information systems in operation, for projects, or for special types of systems or projects. As is illustrated in Figure 2, many of the risk factors that apply to information systems in operation also apply to projects and also apply to any work system, regardless of whether IT is involved. For example, risk factors for any work system include lack of management support, lack of required knowledge and skill, and lack of required resources. These risk factors also apply to projects, but projects have some additional risk factors that do not apply to work systems in general, such as inadequate project schedule and inadequate clarity about project requirements.

Furthermore, throughout the analysis of IS-related risks, many situations involve neither the risk factors nor the negative outcomes that are uniquely associated with information systems. Focusing solely on IS risk ignores the fact that information systems are just one component of a manager’s business environment and that many operational risks are due to the environment in which a system is operating rather than the system itself. For example, security failures are often more related to lax security policies and lax enforcement than to technical capabilities. Limiting the discussion to information systems risk can create a “responsibility gap” in an organization if IS managers are responsible for managing IS risk, and business managers, who should be identifying, assessing, and developing strategies for overall business risk, are left in the dark.

Ideally, risk factors should help managers develop risk management strategies. But there has been little effort to organize risk factors in a manner that is meaningful for managers and that accounts for the existence of risk factors at different levels. We believe that the work system framework, which is based upon a business management model, is an effective tool not only for organizing risks associated with IS, but also as a medium for communication between IS and business managers.

## III. USING THE WORK SYSTEM FRAMEWORK TO ORGANIZE RISK FACTORS

A work system is a system in which human participants and/or machines perform work using information, technologies, and other resources to produce products and/or services for internal or external customers. Figure 3 is a graphical representation of the work system framework [Alter 2002; 2003], which identifies nine elements needed for even a superficial understanding of a work system. The arrows between various elements reflect the importance of mutual alignment among the elements.

The work system framework represents a system in a language that is understandable by business managers, and it can be used to organize the many risk factors in the IS literature. Table 5 demonstrates that the work system framework could serve as a framework for organizing risk factors by associating each of 30 common risk factors with a specific element of a work system Because information systems and projects are special cases of work systems [Alter, 2002; 2003], the risk factors that apply to work systems in general should also apply to information systems and projects as well. For example, a poorly designed business process (the first risk factor for work practices) increases the probability of negative outcomes regardless of whether the focus is a sales information system in operation or the development or implementation phase of an ERP project. The same can be said for the risk factors “inadequate managers and leaders” (listed under participants) and “lack of management support and attention” (listed under environment).

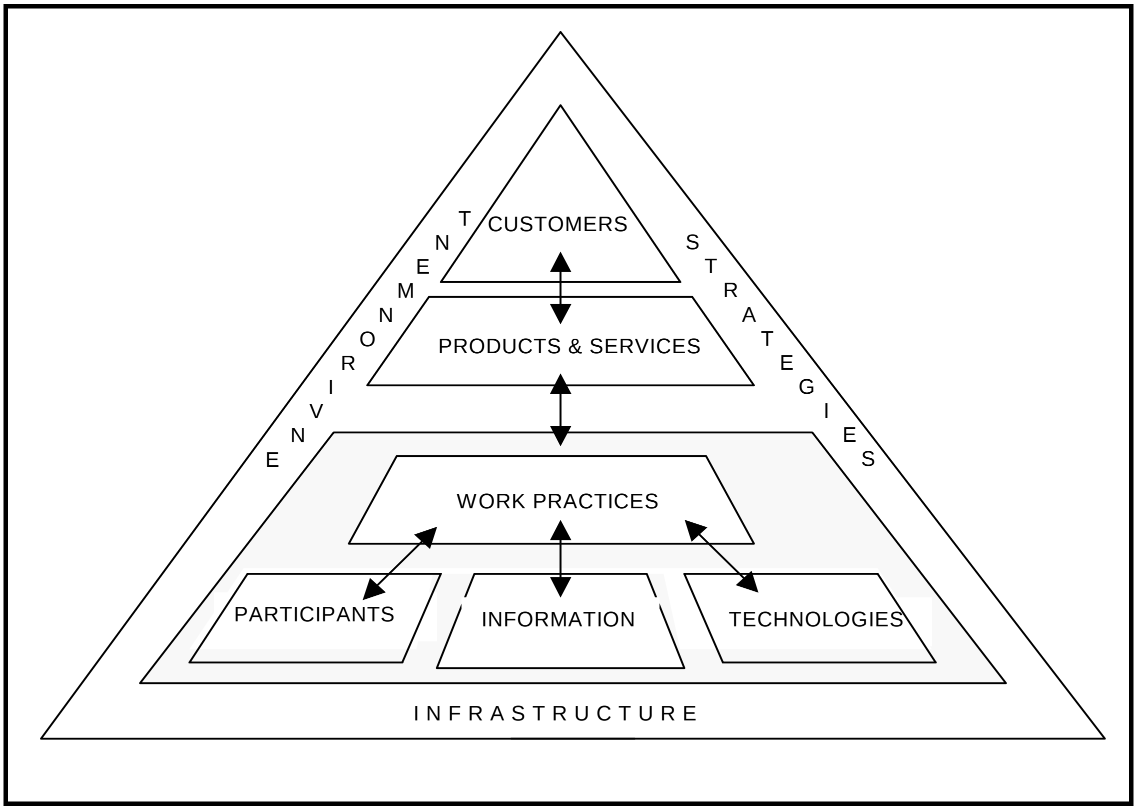



Figure 3. The Work System Framework (as revised in Alter [2003])

Table 5. Risk Factors and Related Negative Outcomes for Systems in Organizations

| ***Work system element*** | ***Typical risk factors and negative outcomes*** |
|---|---|
| Work practices | RISK FACTORS<br>• Poorly designed business process<br>• Inadequate fit of work practices with other work system elements<br>• Inadequate resources to support the work practices<br>• Inadequate planning and control mechanisms within the business process<br><br>NEGATIVE OUTCOMES<br>• Inadequate performance in terms of productivity, consistency, cycle time, activity rate, or other measures |
| Participants | RISK FACTORS<br>• Inadequate managers and leaders<br>• Inadequate skills and understanding<br>• Lack of motivation and interest<br>• Inability or unwillingness to work together to resolve conflicts<br>• Mismatch between characteristics of participants and requirements of the process |

| ***Work system element*** | ***Typical risk factors and negative outcomes*** |
|---|---|
| | NEGATIVE OUTCOMES<br>• Inadequate performance in terms of productivity, consistency, cycle time, activity rate, or other measures<br>• Personnel problems |
| Information | RISK FACTORS<br>• Inadequate information quality<br>• Inadequate information accessibility<br>• Inadequate information presentation<br>• Inadequate information security<br><br>NEGATIVE OUTCOMES<br>• Inadequate business process performance in terms of productivity, consistency, cycle time, activity rate, or other measures<br>• Participant frustration<br>• Information loss or theft |
| Technologies | RISK FACTORS<br>• Technology is difficult and inefficient to use.<br>• Technology performance is inadequate for requirements of business process.<br>• Hardware or software contains serious bugs that could degrade work system efficiency or effectiveness.<br>• Incompatibility of technology with other complementary technologies elsewhere<br><br>NEGATIVE OUTCOMES<br>• Inadequate business process performance in terms of productivity, consistency, cycle time, activity rate, or other measures<br>• Participant frustration |
| Products & Services | RISK FACTORS<br>• The work system produces products or services whose average quality or cost to the customer is inadequate.<br>• The products and services are not what the customers want.<br><br>NEGATIVE OUTCOMES<br>• Customers do not use products or switch to substitutes<br>• Customers complain about poor fit of products to their needs |
| Customers | RISK FACTORS<br>• Disagreement among customers concerning the requirements or expectations for the products and services.<br>• Difficulty using or adapting the work system's products and services.<br><br>NEGATIVE OUTCOMES<br>• Customers do not use products or switch to substitutes<br>• Customers complain about poor fit of products to their needs |
| Environment | RISK FACTORS<br>• Lack of management support and attention<br>• Inconsistencies with the organizational culture<br>• Lack of fit with the demands of the surrounding environment<br>• High level of turmoil and distractions.<br><br>NEGATIVE OUTCOMES<br>• Diminished work system performance due to lack of support or effort drained by environment-related issues. |
| Infrastructure | RISK FACTORS<br>• Human infrastructure inadequate to support the work system. |

| ***Work system element*** | ***Typical risk factors and negative outcomes*** |
|---|---|
| | • Technical infrastructure inadequate to support the work system.<br>• Information system infrastructure inadequate to support the work system.<br><br>NEGATIVE OUTCOMES<br>• Diminished work system performance due to inadequate support from infrastructure. |
| Strategies | RISK FACTORS<br>• Mismatch of the work system with the organization's strategy<br>• Inadequate work system strategy for accomplishing its goals.<br><br>NEGATIVE OUTCOMES<br>• Ineffective work system performance |

## IV. USING ELEMENTS OF THE WORK SYSTEM FRAMEWORK TO ORGANIZE RISK FACTORS

We began our review of the IS risk literature (Section II) assuming that many of the risk factors in the literature would seem equally valid for work systems in general as for information systems or projects or special cases of either. We decided to explore this possibility in some detail because broadly applicable categories of risk factors may facilitate risk management by making available knowledge more readily usable.

Appendix I classifies each of 228 risk factors found in these articles based on the element of the work system framework that we believe is most closely associated with the risk factor. For simplicity of format, Appendix I is divided into nine tables, one for each element of the work system framework[2].

To explore whether many of the risk factors for information systems or projects seem to be equally valid as risk factors at a different level, we further categorized each risk factor based on whether we believe it is applicable at eight different levels[3]. The eight levels are listed in Table 6.

Table 6. Risk Factor Levels

| | |
|---|---|
| WS | Work systems in general (WS in operation) |
| IS | Information systems in general (IS in operation) |
| Project | Projects in general |
| IS Project | Information system project |
| Type of IS | Type of information system (specific type of IS in operation) |
| Type of IS Project | Type of IS-related project (such as an ERP project or reengineering project) |
| SW | Software in operation on a computer |
| SW Project | Software projects (in contrast to IS projects in organizations) |

[2] It is unlikely that any reader would come up with exactly the same primary associations that we agreed on for the risk factors, but we doubt that the overall balance of associations would turn out substantially different among people familiar with the work system framework.

[3] As with the primary associations with work system elements, it is unlikely that any reader will agree 100% with our beliefs about the applicability of 228 risk factors at 8 levels.

The eight columns in the middle of each table in Appendix 1 indicate the levels at which we believe each risk factor applies. Each cell in these columns contains S, B, or blank. "S" identifies the type of work system (e.g., any work system, any project, or a particular type of IS) the authors of the original article were referring to. Wherever "S" appears in several columns for a particular risk factor, different authors mentioned that risk factor in relation to different levels of system or project. "B" within a cell refers to our belief (based on personal experience and familiarity with the literature) that a particular risk factor is relevant to a level of system or project that the article or book's authors were not referring to directly. A blank cell exists wherever we believe the risk factor does not generally apply to a particular level of system or project.

The form and content of Appendix I demonstrate a number of points.

1. *Large number of risk factors.* The extensiveness of the tables demonstrates that a large number of risk factors are discussed in the IS risk literature. Had we selected a larger sample of articles, we would have found an even larger number of risk factors.

2. *Organization using the work system framework is effective.* Most of the risk factors in the literature search could be associated easily with one of the work system elements. Most risk factors that relate to fit between two elements concern the fit between work practices and some other element such as participants, information, or technology. An example is the lack of fit between participant skills and the skills required by the work practices. In such cases, it is usually most effective and meaningful to associate the risk factor with the other element because work practices link to most of the other elements, either explicitly (through arrows in the work system framework) or implicitly.

*3. Many of the most common risk factors in the IS risk literature are not uniquely related to either IS in operation or IS projects.* Table 7 shows how the elements of the work system framework can be used to organize the risk factors in the 46 articles. It shows that over half (134 of 228) are relevant to work systems in general even though the researchers reporting specific risk factors may have focused on a more limited topic, such as a particular type of information system or project. For example, Barki et al [2001] state that lack of expertise with the task is a risk factor related to information systems projects. We believe that this same risk factor is equally applicable to all of the following cases: work systems in general, information systems in general, projects in general, information system projects, particular types of information systems, particular types of

Table 7. Factors That Relate to Work Systems in General

| ***Work System Element*** | ***Number of factors found in the literature survey*** | ***Number of these factors related to work systems in general*** | ***Percentage of these factors related to work systems in general*** |
|---|---|---|---|
| System Participants | 49 | 35 | 71% |
| Information | 12 | 7 | 58 |
| Technology | 24 | 18 | 75 |
| Work Practices | 52 | 23 | 44 |
| Products/services | 9 | 6 | 66 |
| Customers | 33 | 15 | 45 |
| Environment | 22 | 15 | 68 |
| Infrastructure | 10 | 3 | 30 |
| Strategy | 17 | 12 | 71 |
| Total | 228 | 134 | 59% |

information systems projects, and software projects. Similarly, 119 of the 228 risk factors can be associated with information systems in general even though the original authors associated those factors with other topics. In total, B's appeared in 1002 of the 1824 cells in the nine tables in Appendix I.

*4. Possibilities for organizing risk factors for use.* Typical MBA students, and hence typical business managers, can easily visualize the meaning of the work system elements. Consequently, organizing risks and risk factors by associating them with work system elements could help business managers organize and communicate risks and risk factors. This organization would fit directly into the work system method [Alter, 2002] that is being developed to help business professionals analyze systems at whatever level of detail is appropriate for their purposes.

## V. ORGANIZING RISK FACTORS USING THE WORK SYSTEM LIFE CYCLE

The work system framework presents a relatively static view of how a work system operates during a particular time interval in which its form is relatively constant. The next step is to look at how work systems change over time. The work system life cycle (WSLC) model in Figure 4 summarizes how a work system's form evolves through iterations combining planned change through visible projects and unplanned change through incremental adaptations [Alter, 2002; 2003]. Figure 4 identifies the four phases of planned change:

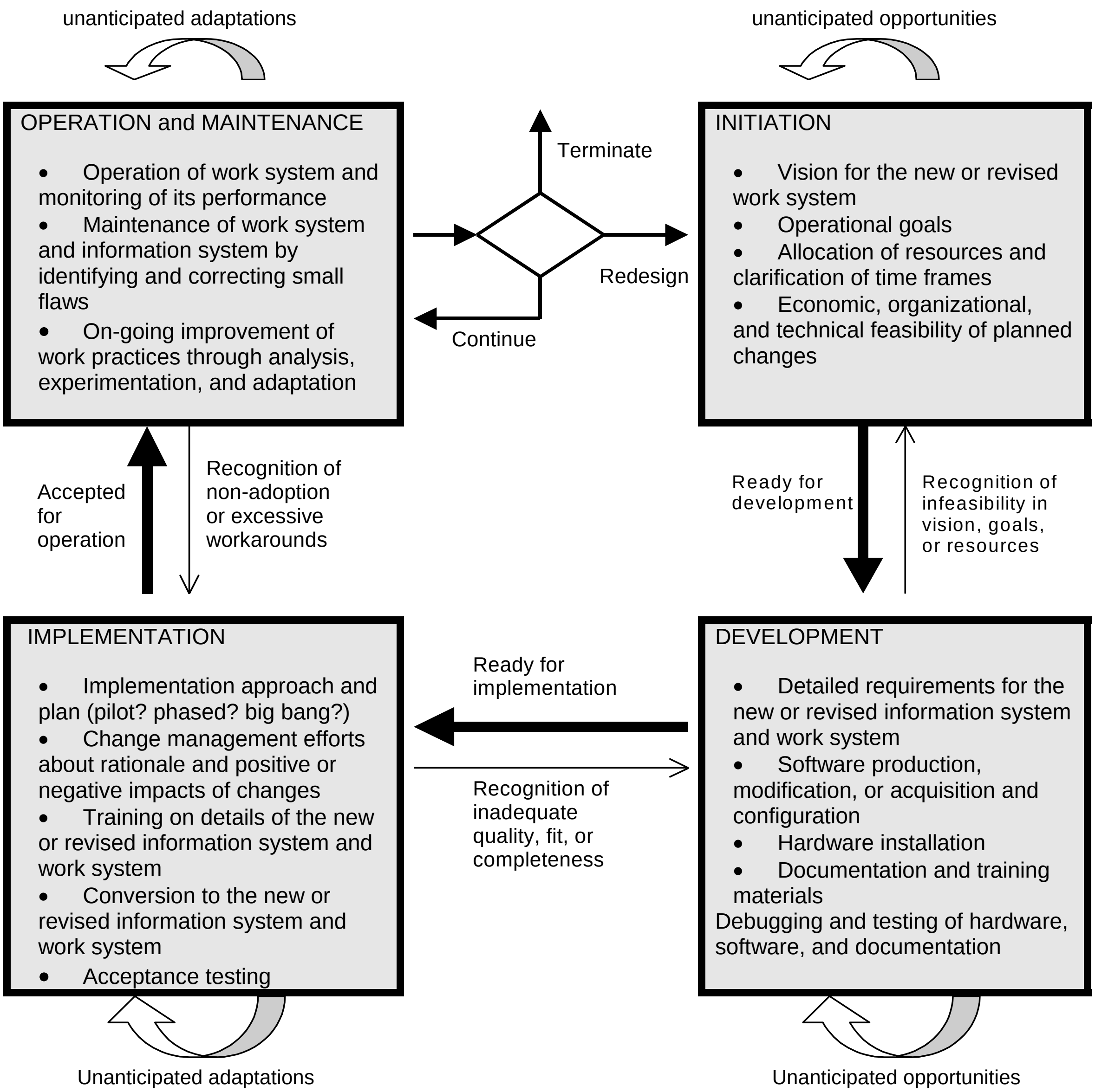
1. operation and maintenance
2. initiation,
3. development,
4. implementation.

Each phase may include unplanned changes based on local experimentation and adaptation. The small, inward directed arrows for each phase in Figure 4 represent the unplanned changes. Each iteration of the model starts with an operation and maintenance phase because relatively few work systems are created from scratch. In most cases, an existing work system is modified or extended to solve problems or exploit opportunities. The WSLC's basic concepts are readily understandable by employed MBA and executive MBA students (who work in responsible managerial positions). They are useful in visualizing reasons for project success and failure when analyzing published case studies and case studies the students write about situations in their own companies.

Just as the elements of the work system framework can be used to organize risk factors in the IS literature, the phases of the WSLC can be used to provide a life cycle-oriented perspective on risk factors. Furthermore, each phase of the WSLC can be viewed as a separate work system and analyzed in terms of the nine work system elements included in the work system framework. The operation and maintenance phase represents a work system in operation. The initiation, development, and implementation phases within an iteration of the WSLC can be viewed as individual projects (and hence work systems) on their own right.

Looking at each of the four phases using the nine work system elements generates 36 separate, but clearly organized categories that can be used for thinking about risks and risk factors. Appendix II illustrates the potential value of this approach:

- It provides four separate tables, one for each phase.
- Each table contains a separate row for each work system element.
- Each row defines the element in reference to the phase and then lists risks that we believe are relevant based on our experience and our reading of the literature.




Source: Alter [2002]

Figure 4. The Work System Life Cycle Model

Unlike the tables in Appendix I, the tables in Appendix II do not attempt to reference each risk factor to specific articles in the literature. Some of the risk factors included in Appendix II did not appear in our literature survey, but we believe they are valid because they make sense in terms of our own experience and are directly linked to the logic of two broadly applicable models, the work system framework and the work system life cycle model. For example, two risks listed for work practices within the implementation phase are "inappropriate implementation approach is selected" and "training materials and training sessions are inadequate and cause disillusionment and other problems." Whether or not those two risks had been included in a list from prior research, we have encountered related problems and believe that a table conveying such risks and risk factors organized by work system element within the four phases of the work system life cycle could be a valuable and easily used tool.

We believe that the difference between risks for the various phases will help clarify the differences in risk profiles between software projects whose immediate goal is to produce debugged software that satisfies requirements versus information system projects whose immediate goal is to improve the operation of work systems in organizations. This approach may also help clarify temporal issues in the study of risks. Some risks such as those related to incomplete requirements and organizational politics grow and emerge across the various phases of the work system life cycle. After identifying risks that affect all parts of the lifecycle, looking at the different phases separately should help in understanding how the emergence and growth of risks in one phase affect the risks in the next phase.

## VI. DISCUSSION AND CONCLUSIONS

This article shows that the IS risk literature produced several hundred risk factors and many overlapping risk components that are difficult for managers to access and use in a meaningful way. Moreover, focus on IS risk sometimes ignores the fact that information systems are just one component of a work system and that many risks and risk factors are associated with other aspects of a work system.

The article shows how the work system framework can be used to categorize risk factors in the IS risk literature. It demonstrated that many of the most important and most commonly cited risk factors for IS in operation and IS projects are actually risk factors for work systems in general. It also showed how the work system life cycle model can be combined with the work system framework to generate a more granular view of risk and risk factors across a work system's history.

The advantages of using the work system framework and the work system life cycle model include:

- Moving toward comprehensive risk assessment
- Organizing risk factors using the work system framework
- Using inheritance to make risk factors more accessible
- Using the work system life cycle to make risk factors more accessible in different stages
- Addressing the "responsibility gap" between IS and business managers.

We will discuss each topic in turn.

*Moving toward comprehensive risk assessment.* As explained in our companion article [Alter and Sherer, 2004], we believe that using work systems as a central concept overcomes some of the limitations of previous IS risk models that are limited to specific aspects of the development process (e.g. software engineering) or system operation (e.g. coordination mechanisms).

1. A work system approach provides a common denominator supporting risk assessment for information systems in operation and for projects and for special cases of each.

2. Especially as information systems are increasingly integrated with and difficult to separate from the work systems they support, it focuses attention on the main goal of risk management: achieving desired results from a work system.

3. Some of the outcomes may be internal to the specific work system being analyzed, whereas other outcomes may involve other work systems that may be information systems or projects.

4. The inclusion of the environment as one of nine work system elements makes it more likely that the surrounding environment will be considered when identifying potential negative outcomes.

*Organizing risk factors using the work system framework.* We identified 228 risk factors in our literature search and showed that each risk factor could be associated with one of the nine elements of a work system. We also showed that over half of the risk factors seemed valid as risk factors for work systems in general even though the original research identified them as risk factors for particular types of information systems or projects. We argued, without proof, that organizing risk factors around work system elements could make them more accessible and usable by managers. It would be of interest to test that assumption by developing a risk management tool or method that helped managers find and apply the relevant risk factors in a highly expeditious way instead of assuming they should know the risk factors intuitively or should be willing to read the IS risk literature or thumb through disorganized lists of risk factors to find those that truly apply to their situation.

*Using inheritance to make risk and risk factors more accessible.* The relationship between risk factors for work systems in general and risk factors for special cases such as projects and IS in operation can become the basis of a hierarchical method for classifying and using risk factors. This would provide economy in codifying and using risk factors. Organized by work system element, the hierarchy would start with risk factors for work systems in general and would identify additional risk factors for projects and information systems. The next level in the hierarchy would identify additional risk factors for special cases of projects and special cases of information systems. The organization via work system elements and the hierarchy should make risk factors more readily accessible and usable.

A possible next step would be to use the hierarchy of risk factors to develop risk diagnostics and tools for improving risk management. Use of the diagnostics in any particular situation would combine relevant risks and risk factors for work systems in general plus additional risks and risk factors associated with the specific type of situation that is being managed. In developing practical risk diagnostics it would be important to verify that those diagnostics fit comfortably into risk management processes that are practical for the types of managers in the relevant situations. It would be of interest to test this assumption by creating and testing tools that use the idea of hierarchy to select and display the risk factors that are appropriate in particular situations.

*Using the work system life cycle model to make risk factors more accessible*. Appendix II shows that the work system life cycle model can be combined with the work system framework to categorize risks and risk factors with greater granularity. Risk factors for work systems in general apply to each phase of the work system life cycle because each phase can be viewed as a separate work system on its own right. On the other hand, some risks factors that apply in a development phase (e.g., risk factors related to the effect of programming techniques on ease of debugging) do not apply in implementation phases. Similarly, risk factors specifically about implementation phases do not apply directly to the other phases. The extensive listing of risks in 36 categories (nine work system elements within each of four phases) demonstrates the potential of organizing risks and risk factors in substantial detail using a model that managers can understand readily. As with the association of risk factors with work system elements and the use of hierarchy (above), future efforts should clarify how the organization of risk and risk factors around system life cycle phases could help in providing risk managers with the most relevant information in the most useful form.

*Addressing the "responsibility gap" between IS and business managers.* Finally, the classification of risks and risks factors could help in addressing the common "responsibility gap" between IT professionals who often justify IT projects and the business managers who are responsible for specific action steps to ensure that benefits in the organization are realized [Sherer et al, 2002]. This article's extensive use of work system concepts was motivated in part by the need to improve communication between business and IT professionals by using ideas and methods that are comfortable for business professionals. Many, perhaps most, risks related to systems in organizations are business risks. It is the ultimate responsibility of business professionals, not IT professionals, to insure that information systems support the business effectively. The acronyms and vocabulary of IT professionals are often confusing and sometimes impenetrable to business professionals responsible for managing organizational risks. Regardless of how clear and logical, vocabulary and methods for helping IT professionals manage software development risks in complex projects probably are not the key to better communication and understanding for business professionals. Better ways of describing risk and relating it to everyday business projects and operations could help substantially. The work system approach presented here focuses on business risks and uses vocabulary that is recognizable and understandable to business professionals. Enabling business and IT to speak the same language supports enhanced communication that is necessary for collaboration between IT and business professionals attempting to reduce IS-related business risks. Effective use of a risk model and careful organization of risk factors should help clarify responsibilities, thereby reducing responsibility gaps that exist in many situations.

*Editor's Note:* This article was received on April 16, 2004 and was published on July 7, 2004.

**REFERENCES**

Alter, S. (2002). "The Work System Method for Understanding Information Systems and Information Systems Research", *Communications of the AIS,* (9)6, pp. 90-104.

Alter, S. (2003). "18 Reasons Why IT-reliant Work Systems Should Replace 'the IT Artifact" as the Core of the IS Field", *Communications of the AIS, (*12)23, pp. 365-394.

Alter, S. and S. A. Sherer (2004). "A General, But Readily Adaptable Model Of Information Systems Risk," *Communications of the AIS,* (14)1, pp. 1-28

Austin, R. (2001). "The Effects Of Time Pressure On Quality In Software Development: An Agency Model", *Information Systems Research,* (12)2, pp. 195-207.

Barki, H., S. Rivard and J. Talbot (1993). "Toward An Assessment Of Software Development Risk", *Journal of Management Information Systems*,(10)2, pp. 203-225.

Barki, H., S. Rivard and J. Talbot (2001). "An Integrative Contingency Model Of Software Project Risk Management," *Journal of Management Information Systems,* (17)4, pp. 37 (33 pgs).

Bashein, B., L. Markus and P. Riley (1994). "Preconditions For BPR Success And How To Prevent Failures", *Information Systems Management,* (11)2, pp. 7-13.

Baskerville, R. and J. Stage (1996). "Controlling Prototype Development Through Risk Analysis," *MIS Quarterly,* (20)4, pp. 481-504.

Benaroch, M. (2002). "Managing Information Technology Investment Risk: A Real Options Perspective", *Journal of Management Information Systems,* (19)2, pp. 43-84.

Boehm, B. (1988). "A Spiral Model Of Software Development And Enhancement", *IEEE Computer*, pp. 61-72.

Boehm, B. (1989). *Software Risk Management*. Washington DC: IEEE Computer Society Press.

Boehm, B. and R. Ross (1989). "Theory-W Software Project Management: Principles And Examples", *IEEE Transactions on Software Engineering*, pp. 902-917.

Chan, S. (2001). "Risky e-Business", *Internal Auditor*, pp. 62-63.

Clemons, E. K. (1991). "Evaluation of Strategic Investments in Information Technology", *Communications of the ACM*, (34)1, pp. 23-36.

Clemons, E. K. (1995). "Using Scenario Analysis to Manage the Strategic Risks of Reengineering", *Sloan Management Review*, pp. 61-71.

Clemons, E. K., M. E. Thatcher and M. Row (1995). "Identifying Sources of Reengineering Failures: A Study of the Behavioral Factors Contributing to Reengineering Risks", *Journal of Management Information Systems,* (12)2, pp. 9-36.

Doherty, N. and M. King (2001). “An Investigation Of The Factors Affecting The Successful Treatment Of Organisational Issues In Systems Development Projects”, *European Journal of Information Systems,* (10), pp. 147-160.

Gogan, J., J. Fedorowicz and A. Rao (1999). “Assessing Risks In Two Projects: A Strategic Opportunity And A Necessary Evil”, *Communications of the AIS,* (1)15.

Grover, V., S. R. Jeong, W. Kettinger and J. Teng (1995). “The Implementation Of Business Process Reengineering”, *Journal of Management Information Systems,* (12)1, pp. 109-144.

Higuera, R. and Y. Haimes (1996). *Software Risk Management*. Pittsburgh: Carnegie Mellon, Software Engineering Institute.

Jiang, J., G. Klein and R. Discenza (2001). “Information System Success As Impacted By Risks And Development Strategies”, *IEEE Transactions on Engineering Management,* (48)1, pp. 46-55.

Jiang, J., G. Klein and T. S. Ellis (2002). “A Measure Of Software Development Risk”, *Project Management Journal,* (33)3, pp. 30-41.

Keil, M., P. Cule, K. Lyytinen and R. Schmidt (1998). “A Framework for Identifying Software Project Risks”, *Communications of the ACM,* (41)11, pp. 76-83.

Kemerer, C. F. and G. I. Sosa (1991). “Systems Development Risks In Strategic Information Systems”, *Information and Software Technology,* (33)3, pp. 212-223.

Kumar, K. and E. Christiaanse (1999). "From Static Supply Chains To Dynamic Supply Webs: Principles For Radical Redesign In The Age Of Information", *Proceedings of ICIS*.

Lee, H. G. and T. Clark (1997). “Market Process Reengineering Through Electronic Market Systems: Opportunities and Challenges", *Journal of Management Information Systems,* (13)3, pp. 113-136.

Loch, K., H. Carr and M. Warkentin (1992). “Threats to Information Systems: Today's Reality, Yesterday's Understanding”, *MIS Quarterly,* (16)2, pp. 173-186.

Lyytinen, K., L. Mathiassen and J. Ropponen (1996). “A Framework For Software Risk Management”, *Journal of Information Technology,* (11), pp. 275-285.

Lyytinen, K., L. Mathiassen and J. Ropponen (1998). “Attention Shaping and Software Risk - A Categorical Analysis of Four Classical R*isk Management Approaches”, Information Systems Research,* (9)3, pp. 233-255.

McComb, D. and J. Y. Smith (1991). “System Project Failure: the Heuristics of Risk”, *Journal of Information Systems,* (8)1, pp. 25-34.

McFarlan, W. (1981). “Portfolio Approach To Information Systems”, *Harvard Business Review,* pp. 142-150.

Mohan, L., W. Holstein and R. Adams (1990). “EIS: It Can Work In The Public Sector”, *MIS Quarterly*, pp. 435-448.

Moynihan, T. (2002). “Coping With Client-Based "People Problems": The Theories of Action of Experienced IS/Software Project Management”, *Information and Management,* (39), pp. 377-390.

Nidumolu, S. (1995). “The Effect Of Coordination and Uncertainty on Software Project Performance: Residual Performance Risk as An Intervening Variable”, *Information Systems Research,* (6)3, pp. 191-219.

Nidumolu, S. (1996). “A Comparison Of Structural Contingency And Risk-Based Perspectives On Coordination In Software Development Projects”, *Journal of Management Information Systems,* (13)2, pp. 77-113.

Rainer, R., C. Snyder and H. Carr (1991). “Risk Analysis for Information Technology”, *Journal of Management Information Systems,* (8)1, pp. 129-147.

Richmond, W. B. and A. Seidmann (1993). “Software Development Outsourcing Contract: Structure And Business Value”, *Journal of Management Information Systems,* (10)1, pp. 57.

Rockart and Crescenzi (1984). "Engaging Top Management In IT," *Sloan Management Review*, pp. 3-16.

Schmidt, R., K. Lyytinen, M. Keil and P. Cule (2001). “Identifying Software Project Risks: An International Delphi Study”, *Journal of Management Information Systems,* (17)4, pp. 5-36.

Scott, J. and I. Vessey (2002). “Managing Risks in Enterprise Systems”, *Communications of the ACM,* (45),4, pp. 74-81.

Sherer, S. (1992). *Software Failure Risk: Measurement and Management*. New York: Plenum Press.

Sherer, S., M. Ray and N. Chowdhury (2002). "Assessing Information Technology Investments with an Integrative Process Framework", *Proceedings of 35th International Conference on System Sciences*, Hawaii.

Smith, H., J. McKeen and D. S. Staples (2001). “Risk Management in Information Systems: Problems and Pitfalls”, *Communications of the AIS,* (7)13.

Straub, D. and R. Welke (1998). “Coping with Systems Risk: Security Planning Models for Management Decision Making”, *MIS Quarterly,* pp. 441-469.

Viehland, D. (2002). “"Risk E-Business": Assessing Risk in Electronic Commerce”, *Decision Line*.

Vitale, M. (1986). “The Growing Risks of Information Systems Success”, *MIS Quarterly,* (10)4, pp. 327-336.

Yourstone, S. and H. Smith (2002). “Managing System Errors and Failures in Health Care Organizations: Suggestions for Practice and Research”, *Health Care Management Review,* (27)1, pp. 50-61.

## APPENDIX I: RISK FACTORS FOUND IN THE LITERATURE, (ORGANIZED USING WORK SYSTEM ELEMENTS) [4]

Table AI-1. Risks Related to System or Project Participants

| ***Risk Factor*** | ***WS*** | ***IS*** | ***Proj*** | ***IS Proj*** | ***Type of IS*** | ***Type of IS Proj*** | ***SW*** | ***SW Proj*** | ***Source*** |
|---|---|---|---|---|---|---|---|---|---|
| Personnel shortfalls | B | B | B | B | B | S | | S | [Boehm 1988; Boehm 1989; Grover et al. 1995] |
| Designer shortcomings | | | B | S | | B | | B | [Lyytinen et al. 1996; Lyytinen et al. 1998] |
| Lack of experience | B | B | B | S | S | B | | B | [Baskerville and Stage 1996; Chan 2001; Grover et al. 1995; McFarlan 1981] |
| Lack of expertise with task | B | B | B | S | B | B | | B | [Barki et al. 1993; Barki et al. 2001; Jiang et al. 2002] |
| Lack of general expertise | B | B | B | S | B | B | | B | [Barki et al. 1993; Barki et al. 2001] |
| Lack of knowledge skills | B | B | B | S | B | B | | B | [Baskerville and Stage 1996; Keil et al. 1998; Schmidt et al. 2001] |
| Lack of application systems expertise | | | | S | | B | | | [Barki et al. 2001; Baskerville and Stage 1996; Jiang et al. 2001; McFarlan 1981] |
| Lack of development expertise | | | | S | | B | | | [Barki et al. 2001] |
| Lack of knowledge of technology | | | | B | | S | | | [Scott and Vessey 2002] |
| Lack of experience with systems development and prototyping | | | | S | | B | | B | [Baskerville and Stage 1996] |
| Manager shortcomings | B | B | B | S | B | B | | B | [Lyytinen et al. 1996; Lyytinen et al. 1998] |
| Lack of effective project management skills | | | B | S | | S | | B | [Grover et al. 1995; Schmidt et al. 2001; Smith et al.2001] |
| Inadequate supplier capabilities | B | B | B | S | B | B | | B | [Smith et al. 2001] |
| New suppliers | B | B | B | S | B | B | | B | [Barki et al. 2001] |
| Lack of external consultant support | B | B | B | B | B | S | | B | [Grover et al. 1995] |
| Vendor problems | B | B | B | B | S | S | B | B | [Kemerer and Sosa 1991] |
| Shortfalls in externally performed tasks | B | B | B | B | B | B | | S | [Boehm and Ross 1989] |
| Inappropriate staffing | B | B | B | S | B | B | | B | [Schmidt et al. 2001] |
| Intensity of conflict | B | B | B | S | B | B | | B | [Barki et al. 1993; Jiang et al. 2002] |

[4] Note: Table 4 in Section IV explains the headings. Table 6 in Section IV summarizes the pattern in the cells of all nine tables in this Appendix.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Team diversity | | | B | S | | B | | | [Barki et al. 1993; Barki et al. 2001] |
| Staffing volatility | B | B | B | S | B | B | | B | [Schmidt et al. 2001] |
| Personnel turnover | B | S | B | B | B | B | | B | [Rainer et al. 1991] |
| Death or injury of personnel | B | S | B | B | B | B | | B | [Rainer et al. 1991] |
| Misunderstanding requirements | | | B | S | | B | B | B | [Keil et al. 1998; Schmidt et al. 2001] |
| Failure to understand customer viewpoints | B | B | B | B | B | S | | B | [Grover et al. 1995] |
| Insufficient understanding of existing data, applications and IT | | | | B | | S | | | [Grover et al. 1995] |
| Inadequate understanding of design specs and computer technology | | | | S | | B | | B | [Baskerville and Stage 1996] |
| Inability to understand human implications of new systems | | | | S | | B | | | [Jiang et al. 2002] |
| Lack of project champion | B | B | B | B | B | S | | B | [Grover et al. 1995] |
| Lack of people skills | B | B | B | S | B | B | | B | [Schmidt et al. 2001] |
| Poor decision making competency | B | B | B | S | B | B | | B | [Smith et al. 2001] |
| Inability to work with uncertain objectives | | | | S | B | B | | B | [Jiang et al. 2002] |
| Difficulty modeling change | | | | B | | S | | | [Grover et al. 1995] |
| Failure to communicate reasons to change | | | | B | | S | | | [Grover et al. 1995] |
| Failure to consider existing culture | B | B | B | B | B | S | | B | [Grover et al. 1995] |
| Inability to work with top mgmt | B | B | B | S | | B | | | [Jiang et al. 2002] |
| Inability to carry out tasks effectively | B | B | B | S | B | B | | B | [Jiang et al. 2002] |
| Poor understanding of company culture | B | B | B | B | B | S | | | [Scott and Vessey 2002] |
| Difficulty gaining cross functional cooperation | B | B | B | B | B | S | | | [Grover et al. 1995] |
| Lack of relationship building | B | B | B | S | B | B | | B | [Smith et al. 2001] |
| Poor team relationships | B | B | B | S | B | S | | B | [Grover et al. 1995; Schmidt et al. 2001] |
| Inability to work as a team | B | B | B | S | B | B | | B | [Jiang et al. 2002] |
| Poor communications | B | B | B | S | B | S | | B | [Grover et al. 1995; Grover et al. 1995; Jiang et al. 2002] |
| Stress | B | S | B | B | B | B | | B | [Yourstone and Smith 2002] |
| Damage or destruction by humans | B | S | B | B | B | B | | B | [Loch et al. 1992; Rainer et al. 1991] |
| Disclosure, modification of data | B | S | B | B | B | B | | B | [Rainer et al. 1991] |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Unauthorized physical access | B | S | B | B | B | B | | B | [Rainer et al. 1991] |
| Unauthorized electronic access | B | S | B | B | B | B | | B | [Rainer et al. 1991] |
| Theft | B | S | B | B | B | B | | B | [Rainer et al. 1991] |

Note: Proj. = Project

Table AI-2. Risks Related to Information

| ***Risk Factor*** | ***WS*** | ***IS*** | ***Proj*** | ***IS Proj*** | ***Type of IS*** | ***Type of IS Proj*** | ***SW*** | ***SW Proj*** | ***Source*** |
|---|---|---|---|---|---|---|---|---|---|
| Project size [too much information] | | | B | S | | B | | B | [McFarlan 1981] |
| Application size | | B | B | S | B | B | | B | [Jiang et al. 2001] |
| Information overload | B | B | B | B | S | B | | B | [Yourstone and Smith 2002] |
| Insufficient documentation of development environment | | B | B | S | | B | | B | [Baskerville and Stage 1996] |
| Poor information about project inputs and outcomes | | | B | S | | B | | B | [Nidumolu 1995] |
| New unfamiliar subject matter | B | B | B | S | B | B | | B | [Schmidt et al. 2001] |
| Problematic data conversion | B | B | B | B | B | S | | B | [Scott and Vessey 2002] |
| Ambiguous and inconsistent system requirements | | | B | S | B | B | | B | [Baskerville and Stage 1996] |
| System interdependence | B | B | B | S | B | B | | B | [Barki et al. 1993; Barki et al. 2001; Gogan et al. 1999] |
| External dependencies not met | B | B | B | S | B | B | | B | [Schmidt et al. 2001] |
| Problematic interfaces | B | B | B | B | B | S | | B | [Scott and Vessey 2002] |
| Information asymmetry in collaboration | B | B | B | B | S | B | | B | [Kumar and Christiaanse 1999; Lee and Clark 1997] |

Table AI-3. Risks Related to Technology

| ***Risk Factor*** | ***WS*** | ***IS*** | ***Proj*** | ***IS Proj*** | ***Type of IS*** | ***Type of IS Proj*** | ***SW*** | ***SW Proj*** | ***Source*** |
|---|---|---|---|---|---|---|---|---|---|
| New technology | B | B | B | S | B | B | B | B | [Barki et al. 1993; Barki et al. 2001; Jiang et al. 2001; Jiang et al. 2002; Keil et al. 1998; McComb and Smith 1991; Schmidt et al. 2001; Smith et al. 2001] |
| Leading edge technology | B | S | B | B | B | B | B | B | [Kemerer and Sosa 1991] |
| New software | B | B | B | S | B | B | S | B | [Barki et al. 1993; Barki et al. 2001; Jiang et al. 2002] |
| Unproven technology | B | B | B | B | S | B | B | B | [Chan 2001] |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Goldplating | B | B | B | B | B | B | B | S | [Boehm and Ross 1989] |
| Straining computer science capabilities | | | | B | B | B | S | S | [Barki et al. 2001; Boehm 1988; Boehm 1989] |
| Excessive computer systems performance and network data communication requirements | | | | S | B | B | B | B | [Baskerville and Stage 1996] |
| Inadequate development tools and technical platform | B | B | B | S | B | B | B | B | [Lyytinen et al. 1996; Lyytinen et al. 1998] |
| Real time performance shortfalls | | | | B | B | B | S | S | [Boehm and Ross 1989] |
| Equipment failure | B | S | B | B | B | B | B | B | [Rainer et al. 1991] |
| Failure to track or adapt to technological changes | B | S | B | B | B | B | B | B | [Vitale 1986] |
| Poor fit of technology to business needs | B | B | B | B | B | S | B | B | [Scott and Vessey 2002] |
| Lack of technology usability | B | S | B | S | B | B | B | B | [Smith et al. 2001] |
| Technical infeasibility | B | B | B | B | S | B | B | B | [Kemerer and Sosa 1991] |
| Instability of technical architecture | B | S | B | S | B | B | B | B | [Schmidt et al. 2001] |
| System interdependence | B | S | B | S | B | B | B | B | [Barki et al. 2001; Gogan et al. 1999] |
| Linkages to externally controlled technologies | B | B | | S | B | B | B | B | [Baskerville and Stage 1996] |
| Shortfalls in externally furnished components | B | B | B | B | B | B | B | S | [Boehm and Ross 1989] |
| Technical complexity | B | B | B | S | B | B | B | B | [Barki et al. 1993; Barki et al. 2001] |
| Database with interactive processing | | | | S | B | B | B | B | [Baskerville and Stage 1996] |
| Computer system incompatible with development environment | | | | S | B | B | B | B | [Baskerville and Stage 1996] |
| Unreliability in large computing machinery | | | | S | B | B | B | B | [Baskerville and Stage 1996] |
| Unreliable software | B | B | B | S | B | B | S | B | [Baskerville and Stage 1996] |
| Software errors | B | B | B | B | B | B | S | S | [Sherer 1992] |

Table A1-4. Risks Related to Work Practices

| ***Risk Factor*** | ***WS*** | ***IS*** | ***Proj*** | ***IS Proj*** | ***Type of IS*** | ***Type of IS Proj*** | ***SW*** | ***SW Proj*** | ***Source*** |
|---|---|---|---|---|---|---|---|---|---|
| Project size [number of processes affected] | | | B | S | | B | B | B | [Barki et al. 1993; McFarlan 1981] |
| Inadequate project structure | | | B | S | | B | | B | [McFarlan 1981] |
| Number of participants | | | B | S | | B | | B | [Barki et al. 1993; Barki et al. 2001; Jiang et al. 2001; Jiang et al. 2002] |
| Extent of changes | | | B | S | | B | | B | [Barki et al. 1993; Barki et al. 2001; Jiang et al. 2002] |
| Insufficient staffing | B | B | B | S | B | B | | B | [Keil et al. 1998; Jiang et al. 2002] |
| Number of user tasks that will be modified | | | B | S | | B | | | [Jiang et al. 2002] |
| Number of hardware/software suppliers | | | B | S | | B | | B | [Barki et al. 1993; Barki et al. 2001] |
| Proximity to core competencies | B | B | B | S | B | B | B | B | [Smith et al. 2001] |
| Poor scope | | | B | B | | S | | B | [Grover et al. 1995] |
| Inability to review proposed design specs | | | B | S | | B | | B | [Baskerville and Stage 1996] |
| Task complexity | B | B | B | S | B | B | B | B | [Barki et al. 1993; Barki et al. 2001] |
| New development process | | | B | S | | B | | B | [Schmidt et al. 2001] |
| Need to reengineer processes | | | B | B | | S | | B | [Scott and Vessey 2002] |
| Difficulty integrating application vendors and subcontractors | | | B | S | | B | | B | [Schmidt et al. 2001] |
| Contract structure | B | B | B | B | B | B | B | S | [Richmond and Seidmann 1993] |
| Lack of appropriate methodology | B | B | B | B | B | S | B | B | [Grover et al. 1995] |
| Lack of effective development process | | | B | S | | B | | B | [Schmidt et al. 2001] |
| Wrong development strategy | | | B | S | | B | | B | [Schmidt et al. 2001] |
| No planning or inadequate planning | B | B | B | S | B | S | B | B | [Grover et al. 1995; Schmidt et al. 2001] |
| Failure to anticipate and plan for change resistance | | | B | B | | S | | | [Grover et al. 1995] |
| Failure to get project plan approval | | | B | S | | B | | | [Schmidt et al. 2001] |
| Too much emphasis on existing process | | | B | B | | S | | B | [Grover et al. 1995] |
| Inadequate project resource mgmt | | | B | S | | S | | B | [Barki et al. 1993; McComb and Smith 1991; Scott and Vessey 2002; Smith et al. 2001] |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Poor or nonexistent control | B | B | B | S | B | S | B | B | [Grover et al. 1995; Schmidt et al. 2001; Scott and Vessey 2002] |
| Poor risk management | B | B | B | S | B | B | B | B | [Schmidt et al. 2001] |
| Poor change management | | | B | S | | B | | | [McComb and Smith 1991; Schmidt et al. 2001; Scott and Vessey 2002] |
| Taking shortcuts | B | B | B | B | B | B | B | S | [Austin 2001] |
| Failure to consider politics | B | B | B | B | B | S | | | [Grover et al. 1995] |
| Poor expectations management | B | B | B | S | B | B | | B | [Keil et al. 1998; Schmidt et al. 2001; Smith et al. 2001] |
| Failure to gain user commitment | B | B | B | S | B | B | | B | [Keil et al. 1998; Schmidt et al. 2001] |
| Failure to identify all stakeholders | B | B | B | S | B | B | | B | [Schmidt et al. 2001] |
| Managing multiple relationships with stakeholders | B | B | B | S | B | B | | B | [Schmidt et al. 2001] |
| Lack of IS participation in reengineering projects | | | B | B | | S | | | [Grover et al. 1995] |
| Failure to include process owners | | | B | B | | S | | | [Grover et al. 1995] |
| Excessive use of outside consultants | | | B | S | | B | | B | [Schmidt et al. 2001] |
| Lack of control over consultants | | | B | S | | B | | B | [McComb and Smith 1991; Schmidt et al. 2001] |
| Failure to match pace of change with staff ability to cope | | | B | S | | B | | | [Smith et al. 2001] |
| Improper definition of roles | | | B | S | | B | | B | [Schmidt et al. 2001] |
| Lack of clarity of tasks | B | B | B | S | B | B | | B | [Baskerville and Stage 1996] |
| Lack of clear role definitions | B | B | B | S | B | B | | B | [Barki et al. 1993; Barki et al. 2001; Jiang et al. 2002] |
| Poor feedback and motivation | B | B | B | S | B | B | | B | [McComb and Smith 1991] |
| Inadequate governance | B | B | B | B | S | B | | B | [Chan 2001] |
| Ambiguity in job expectations | B | B | B | B | B | S | | B | [Grover et al. 1995] |
| Unclear boundaries | B | B | B | S | B | B | | B | [Baskerville and Stage 1996] |
| Focusing only on easily measurable evaluation criteria | B | B | B | B | B | S | | B | [Grover et al. 1995] |
| Artificial deadlines | | | B | S | | B | | B | [Schmidt et al. 2001] |
| Bad estimation | B | B | B | S | B | B | | B | [Schmidt et al. 2001] |
| Long hours | B | B | B | B | S | B | | B | [Yourstone and Smith 2002] |
| HR policies not changed | | | B | B | | S | | B | [Grover et al. 1995] |
| Lack of appropriate employee compensation incentives | B | B | B | B | B | S | | B | [Grover et al. 1995] |
| Under-funded projects | | | B | S | | S | | B | [Jiang et al. 2002; Kemerer and Sosa 1991; Schmidt et al. 2001] |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Under-funding development and maintenance | | | | S | | | | | [Schmidt et al. 2001] |

Table AI-5. Risks Related to the Products and Services Produced

| ***Risk Factor*** | ***WS*** | ***IS*** | **Proj** | ***IS Proj*** | ***Type of IS*** | ***Type of IS Proj*** | ***SW*** | ***SW Proj*** | ***Source*** |
|---|---|---|---|---|---|---|---|---|---|
| Unanticipated results | B | B | B | S | B | B | | B | [Smith et al. 2001] |
| New unfamiliar subject matter | B | B | B | S | B | B | | B | [Schmidt et al. 2001] |
| Leading edge idea | B | B | B | S | B | B | | B | [Kemerer and Sosa 1991] |
| [Inadequate] goals and deliverables | B | B | B | S | B | B | | B | [Lyytinen et al. 1996; Lyytinen et al. 1998] |
| Complex objects with complex relationships | B | B | B | S | B | B | | B | [Baskerville and Stage 1996] |
| Application complexity | | | | S | B | B | B | B | [Jiang et al. 2002] |
| Complex demands | B | B | B | B | S | B | | B | [Yourstone and Smith 2002] |
| Number of links to existing and future systems | | | B | S | | B | | B | [Jiang et al. 2002] |
| Difficulty estimating project performance | | | B | S | | B | | B | [Nidumolu 1995] |

Table AI-6. Risks Related to Customers

| ***Risk Factor*** | ***WS*** | ***IS*** | ***Proj*** | ***IS Proj*** | ***Type of IS*** | ***Type of IS Proj*** | ***SW*** | ***SW Proj*** | ***Source*** |
|---|---|---|---|---|---|---|---|---|---|
| Number of organizational units involved | B | B | B | S | B | B | B | B | [Schmidt et al. 2001] |
| Large number stakeholders | B | B | B | S | B | B | | B | [Jiang et al. 2002] |
| Number of users | | | B | S | | B | | B | [Barki et al. 1993; Barki et al. 2001; Lyytinen et al. 1996; Lyytinen et al. 1998; Jiang et al. 2002] |
| Number of hierarchical levels occupied by users | | | B | S | | B | | B | [Barki et al. 1993; Barki et al. 2001] |
| Large number of levels of users | | | B | S | | B | | B | [Jiang et al. 2002] |
| Oversubscription | B | B | B | B | S | B | | B | [Kemerer and Sosa 1991] |
| Unclear scope | B | B | B | S | | B | | B | [Schmidt et al. 2001] |
| Uncertain requirements | B | B | B | S | | B | | B | [Nidumolu 1996] |
| Changing scope | B | B | B | S | | B | | S | [Boehm and Ross 1989; Keil et al. 1998; Schmidt et al. 2001] |
| Lack of frozen requirements | | | B | S | | B | | B | [Keil et al. 1998; Schmidt et al. 2001]; |
| Continuing stream of changes by users | | | B | S | | B | | B | [Boehm and Ross 1989] |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| [Inadequate] customer capability | B | B | B | S | B | B | | B | [Smith et al. 2001] |
| User capability | | | B | S | | B | | B | [Smith et al. 2001] |
| Lack of user experience and support | | | B | S | | B | | B | [Barki et al. 1993; Barki et al. 2001; Jiang et al. 2001; Jiang et al. 2002; Schmidt et al. 2001] |
| Personal deficiencies on part of the customers project mgr | | | B | S | | B | | B | [Moynihan 2002] |
| Ineffective champion | B | B | B | B | B | S | | B | [Scott and Vessey 2002] |
| Unrealistic customer expectations | B | B | B | S | B | S | | B | [Bashein et al. 1994; Grover et al. 1995; Moynihan 2002] |
| Sophisticated users with too high expectations | | | B | S | | B | | B | [Schmidt et al. 2001] |
| Unrealistic schedules/budgets | B | B | B | B | B | B | B | S | [Boehm 1988; Boehm 1989] |
| Disagreement within customer community on project goals | | | B | S | | B | | B | [Moynihan 2002] |
| Inability to describe application and problem | | | B | S | | B | | B | [Baskerville and Stage 1996] |
| Lack of customer ownership | B | B | B | S | B | B | | B | [Moynihan 2002; Schmidt et al. 2001] |
| Lack of adequate user involvement | | | B | S | | B | | B | [Keil et al. 1998; Schmidt et al. 2001] |
| Lack of cooperation from users | | | B | S | | B | | B | [Schmidt et al. 2001] |
| Presence of hidden agendas or conflicts | B | B | B | S | B | B | | B | [Barki et al. 2001; Moynihan 2002; Schmidt et al. 2001] |
| Conflicts between user departments | | | B | S | | B | | B | [Keil et al. 1998; Schmidt et al. 2001] |
| Resistance to change | | | B | B | | S | | | [Bashein et al. 1994] |
| Not recognizing need to change | | | B | B | | S | | | [Grover et al. 1995] |
| Failure to commit to new values | | | B | B | | S | | | [Grover et al. 1995] |
| Cultural misunderstandings | B | B | B | B | S | B | | B | [Kumar and Christiaanse 1999] |
| Inadequate training | B | B | B | S | B | S | | B | [Grover et al. 1995; Smith et al. 2001] |
| Inadequate user training | | | B | S | | B | | B | [Smith et al. 2001] |
| Damage or destruction by humans | B | S | B | B | B | B | | B | [Loch et al. 1992; Rainer et al. 1991; ] |

Table AI-7. Risks Related to the Environment

| ***Risk Factor*** | ***WS*** | ***IS*** | ***Proj*** | ***IS Proj*** | ***Type of IS*** | ***Type of IS Proj*** | ***SW*** | ***SW Proj*** | ***Source*** |
|---|---|---|---|---|---|---|---|---|---|
| Difficult to forecast requirements | | | B | B | | S | | | [Grover et al. 1995] |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Difficulty justifying benefits | | | B | B | | S | | | [Grover et al. 1995] |
| Lack of top management support and understanding | B | B | B | S | B | S | B | B | [Bashein et al. 1994; Grover et al. 1995; Keil et al. 1998; Mohan et al. 1990; Schmidt et al. 2001] |
| Change in ownership or senior management | B | B | B | S | B | B | B | B | [Schmidt et al. 2001] |
| Climate of change | | | B | S | | B | | | [Schmidt et al. 2001] |
| Mismatch between company culture and required changes | | | B | S | | B | | | [Schmidt et al. 2001] |
| Unstable corporate environment | B | B | B | S | B | B | B | B | [Schmidt et al. 2001] |
| No market | B | B | | | S | | | | [Kemerer and Sosa 1991] |
| Interorganizational problems | B | B | B | B | S | S | B | B | [Kemerer and Sosa 1991] |
| Competitor copies system | B | B | | | S | | | | [Kemerer and Sosa 1991] |
| High exit barriers | B | B | | | S | | | | [Kemerer and Sosa 1991] |
| Unstable competitive, collaborative, or cooperative environment | B | B | B | B | B | S | | B | [Scott and Vessey 2002] |
| Difficulty measuring performance | B | B | B | B | B | S | B | B | [Grover et al. 1995] |
| Failure to continually assess emerging IT | | B | | B | B | S | B | | [Grover et al. 1995] |
| Contaminants | B | S | | | | | | | [Rainer et al. 1991] |
| Bad Weather | B | S | | | | | | | [Rainer et al. 1991] |
| Fire | B | S | | | | | | | [Rainer et al. 1991] |
| Humidity | B | S | | | | | | | [Rainer et al. 1991] |
| Unauthorized physical access | B | S | | | | | | | [Loch et al. 1992; Rainer et al. 1991]] |
| Theft | B | S | | | | | | | [Rainer et al. 1991] |
| Hackers, viruses, EDI fraud | | | | | S | | | | [Rainer et al. 1991] |
| Voice mail fraud | | | | | S | | | | [Rainer et al. 1991] |

Table AI-8. Risks Related to the Infrastructure

| ***Risk Factor*** | ***WS*** | ***IS*** | ***Proj*** | ***IS Proj*** | ***Type of IS*** | ***Type of IS Proj*** | ***SW*** | ***SW Proj*** | ***Source*** |
|---|---|---|---|---|---|---|---|---|---|
| Organizational and institutional structure | B | B | B | S | B | S | | B | [Lyytinen et al. 1996; Lyytinen et al. 1998; Scott and Vessey 2002] |
| Rigid hierarchical structures | | | B | B | | S | | | [Grover et al. 1995] |
| Organizational inflexibility | B | B | B | B | S | S | | B | [Kemerer and Sosa 1991] |
| Inability to implement with available technical environment | | | | S | | B | | B | [Baskerville and Stage 1996] |
| ERP infrastructure problems | | | | B | B | S | | | [Scott and Vessey 2002] |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Limited telecommunications infrastructure | | | | B | | S | | | [Grover et al. 1995] |
| Telecom problems | | B | | B | S | S | | | [Kemerer and Sosa 1991] |
| Limited database infrastructure | | | | B | B | S | | | [Grover et al. 1995] |
| Poor help desk and support problems | | B | | S | B | B | | | [Smith et al. 2001] |
| Power interruption | B | S | | | | | | | [Rainer et al. 1991] |

Table A1-9. Risks Related to Strategy

| ***Risk Factor*** | ***WS*** | ***IS*** | ***Proj*** | ***IS Proj*** | ***Type of IS*** | ***Type of IS Proj*** | ***SW*** | ***SW Proj*** | ***Source*** |
|---|---|---|---|---|---|---|---|---|---|
| Lack of clarity of success factors and measures | B | B | B | S | B | B | | B | [Smith et al. 2001] |
| Resource insufficiency | B | B | B | S | B | B | | B | [Barki et al. 2001; Grover et al. 1995] |
| Preemption of project by higher priority | | | B | S | | B | | B | [Schmidt et al. 2001] |
| Time constraints | B | B | B | S | B | B | | B | [Gogan et al. 1999] |
| Organizational alignment | B | B | B | S | | B | | | [Doherty and King 2001] |
| Lack of strategic vision | B | B | B | B | | S | | | [Grover et al. 1995] |
| Poor strategic vision | B | B | B | B | B | S | | B | [Scott and Vessey 2002] |
| Project not based on sound business case | | | B | S | | B | | B | [Schmidt et al. 2001] |
| Trying change either too radical or not radical enough | | | B | B | | S | | B | [Grover et al. 1995] |
| Top management has short term view | B | B | B | B | B | S | | | [Grover et al. 1995] |
| Projects intended to fail | | | B | S | | B | | B | [Schmidt et al. 2001] |
| Lack of alignment between corporate and IT planning | | B | B | B | B | S | | B | [Grover et al. 1995] |
| Loss of resource control | B | B | B | B | S | B | | B | [Kumar and Christiaanse 1999] |
| Changing competitive forces | B | B | B | B | S | B | | | [Vitale 1986] |
| Increasing supplier/customer power | B | B | B | B | S | B | | | [Viehland 2002] |
| Changing basis of competition | B | B | B | B | S | B | | | [Viehland 2002] |
| Bad timing | B | B | B | B | S | B | | | [Viehland 2002] |

## APPENDIX II: RISKS RELATED TO PHASES IN THE WORK SYSTEM LIFE CYCLE (ORGANIZED BY PHASE AND WORK SYSTEM ELEMENT)

Table A2-1: Risks during the Operation and Maintenance Phase for any Work System

| | | |
|---|---|---|
| Operation & Maintenance | Work Practices | The operation and maintenance phase includes:<br>• Operate and monitor the work system<br>• Perform maintenance by fixing flaws and creating minor improvements<br>• Perform continuous improvement of work practices through analysis, experimentation, and adaptation.<br><br><u>RISKS:</u><br>• Failure to operate the business process efficiently or effectively.<br>• Failure to maintain the work system, resulting in gradual degradation of work system performance.<br>• Inadequate fit of the business process with other work system elements<br>• Inadequate resources to support the business processes<br>• Ineffective operational management and leadership |
| Operation & Maintenance | Participants | Participants include people who perform the work done by the business process and people who maintain the work system.<br><br><u>RISKS:</u><br>• Inadequate managers and leaders<br>• Inadequate skills and understanding<br>• Lack of motivation and interest [typically resulting in poor quality, lower productivity, higher rework.)<br>• Inability or unwillingness to work together to resolve conflicts<br>• Errors by participants: poor judgment in making decisions, operator error in using technology<br>• Mismatch between characteristics of participants and requirements of the process |
| Operation & Maintenance | Information | Information is the codified and non-codified information used or generated as participants perform their work<br><br><u>RISKS:</u><br>• Inadequate information quality (Data errors degrade system operation; Incorrect or untimely data produced by the system.)<br>• Inadequate information accessibility<br>• Inadequate information presentation<br>• Inadequate information security |
| Operation & Maintenance | Technologies | The tools and techniques work system participants use while performing their work.<br><br><u>RISKS:</u><br>• Technology is difficult and inefficient to use.<br>• Technology crashes.<br>• Technology performance is inadequate<br>• Hardware or software bugs degrade work system efficiency or effectiveness.<br>• Incompatibility of technology with other complementary technologies elsewhere.<br>• Difficulty maintaining the technology |
| Operation & Maintenance | Products & Services | The products and services the work system produces for its customers.<br><br><u>RISKS:</u><br>• The work system produces products or services whose average quality or cost to the customer is inadequate.<br>• Particular instances of the work system's products or services contain major flaws. |

| | | |
|---|---|---|
| Operation & Maintenance | Customers | People who receive direct benefits from products and services the work system produces<br><br>RISKS:<br><br>• New or modified work system produces products and services that its customers don't want.<br>• Work system customers change, and new customer requirements differ from previous customer requirements.<br>• Major flaws in particular instances of the work system's products or services cause significant problems for customers. |
| Operation & Maintenance | Environment | Organizational, cultural, competitive, technical, and regulatory environment within which the work system operates.<br><br>RISKS:<br><br>• Lack of management support and attention needed for effective operation of the work system.<br>• Inconsistencies with the organizational culture undermine work system performance.<br>• High level of turmoil and distractions undermines work system performance.<br>• Changes in the surrounding environment dictate that the new or modified work system is no longer adequate. |
| Operation & Maintenance | Infrastructure | Human, informational, and technical resources that the work system relies on even though these resources exist and are managed outside of it and are shared with other work systems<br><br>RISKS:<br><br>• Human, technical, or informational infrastructure is inadequate to support the ongoing operation and maintenance of the new or modified work system.<br>• Particular failures of human, technical, or informational infrastructure degrades or prevents work system operation during a particular period |
| Operation & Maintenance | Strategies | The rationale under which the work system operates, plus the strategies of the business function, IT group, and entire firm.<br><br>RISKS:<br><br>• The organization's strategy changes, creating or exacerbating a mismatch with the work system's strategy. |

Table A2-2: Risks During the Initiation Phase for any Work System

| | | |
|---|---|---|
| Initiation | Work Practices | The initiation phase includes determining the vision for the new work system; operational goals; allocation of resources and clarification of time frames; economic, organizational, and technical feasibility<br><br>RISKS:<br><br>• Inadequate process (not enough attention, understanding, involvement) |
| Initiation | Participants | People who participate in the initiation phase. Typically these should include representatives of the relevant business functions, the IT group, and other stakeholders.<br><br>RISKS:<br><br>• Key stakeholders not included in deliberations.<br>• Key stakeholders unwilling or unable to participate in deliberations. |

| | | |
|---|---|---|
| Initiation | Information | Information used in the initiation phase. This includes the general form and operation of relevant systems, difficulties with the existing systems, new opportunities, goals, wish lists, and available resources.<br><br>RISKS:<br><br>• Important facts overlooked<br>• Social and organizational issues not considered as information<br>• Unwarranted assumptions about technology that might be used in the target system or in the development of software<br>• Infrastructure and environmental issues not considered adequately. |
| Initiation | Technology | The technology used during the initiation phase. Typically a non-issue except where conferencing might help virtual teams.<br><br>RISKS:<br><br>• (Nothing specific to technology during the initiation phase) |
| Initiation | Products & Services | The initiation phase produces a formal or informal functional specification that summarizes the types of changes that are desired. It also produces a project plan including an overview schedule and allocation of resources to the development and implementation phases.<br><br>RISKS:<br><br>• Functional requirements produced are misdirected<br>• Functional requirements produced are over-ambitious and exceed the organization's ability to change<br>• Requirements produced are not fully understood.<br>• Project plan produced in the initiation phase is unrealistic or extremely difficult in terms of schedule, resources, and production goals. |
| Initiation | Customers | The customers of the initiation phase include the business function that will operate the new work system, the IT group that will produce or configure the hardware and software, and the entire team of people who will work in the development phase.<br><br>RISKS:<br><br>• Project designed for wrong customer (e.g., a manager dictates part of the requirements without sufficient analysis or thought)<br>• Too much attention to goals of a single customer (e.g., insufficient attention to the needs of a second functional area or to the quality requirements of the IT group) |
| Initiation | Environment | Organizational, cultural, competitive, technical, and regulatory environment within which the initiation phase will occur and within which the new or modified work system will be developed and implemented.<br><br>RISKS:<br><br>• Inadequate consideration of environmental factors such as regulatory requirements, competitive issues, and organizational culture.<br>• Initiation during a crisis situation in which speed overrides care in deciding big picture changes<br>• These environment-related risks apply for all phases of a project:<br>- Lack of management commitment<br>- Management unwillingness to allocate necessary resources<br>- Lack of consensus on the need for the project<br>- Lack of consensus about project governance<br>- Culture of ineffective cooperation on projects |
| Initiation | Infrastructure | Human, informational, and technical resources that the initiation phase will rely on even though these resources exist and are managed outside of the work done in the initiation phase. |

| | | |
|---|---|---|
| | | RISKS:<br><br>• (Nothing specific to infrastructure during the initiation phase) |
| Initiation | Strategies | The rationale under which the initiation phase is performed, plus the strategy of the business function, IT group, and entire firm.<br><br>RISKS:<br><br>• The strategy of the initiation phase is flawed (e.g., too little effort to consider needs and issues of different stakeholders)<br>• The requirements produced are partly or largely inconsistent with the organization's strategy. |

Table A2-3: Risks During the Development Phase for any Work System

| | | |
|---|---|---|
| Development | Work Practices | The development phase includes:<br><br>• Detailed requirements for the new or revised information system and work system<br>• Software production, modification, or acquisition and configuration<br>• Hardware installation<br>• Documentation and training materials for technical and non-technical aspects of the work system.<br>• Debugging and testing of hardware, software, and documentation<br><br>RISKS:<br><br>• Error prone development process<br>• Overly costly or overly complex development process<br>• Analysis paralysis<br>• Excessive fixation on the schedule<br>• Excessive fixation on the method rather than the results.<br>• Inadequate experimentation and proof of concept.<br>• Inadequate attention to documentation and training materials<br>• Incomplete debugging and testing |
| Development | Participants | Participants include business representatives, business analysts, programmers, technical architects, technical writers, and others.<br><br>RISKS:<br><br>• Participants who are not fully able to perform the work needed for successful development. (e.g., user representatives who are not senior enough to make judgments about what might or might not work)<br>• Non-engaged participants do slipshod work (e.g., programmers who don't care very much about long term quality issues)<br>• Participants not suited to the business process chosen for the project even though they might be able to perform well in a different process (e.g., coders who can't keep up with a prototyping effort)<br>• Participants have too little experience with the technology used in the development process.<br>• Wrong balance between business and IT professionals (e.g., design the process to give too much weight to IT professionals)<br>• Skepticism about whether the project can be done within the allotted time and resources<br>• Inadequate availability of subject matter experts<br>• Fear that the new work system changes will lead to staff reductions and de-skilling |
| Development | Information | Information in the development phase includes the functional specification and plan from the initiation phase, the information gathered to determine detailed requirements, the detailed |

| | | |
|---|---|---|
| | | requirements themselves, and programs and program related information.<br><br><u>RISKS:</u><br><br>• Beginning development from unclear or otherwise inadequate goals and functional requirements<br>• Information gathered or generated in detailed requirements analysis is inaccurate or incomplete.<br>• Information is not considered in enough depth or is ignored altogether.<br>• Inadequate consideration to selecting the right technology for the information system being created or modified. |
| Development | Technologies | Includes the technologies used for developing software (e.g., operating system, DBMS, modeling tools), plus any other technology used in the system development phase.<br><br><u>RISKS</u><br><br>• Inadequate technology used for development process that was chosen (e.g., wrong programming language, inadequate debuggers, etc.) |
| Development | Products & Services | The products and services the development phase produces.<br><br><u>RISKS:</u><br><br>• Development phase produces flawed software or installs inadequate hardware.<br>• Development phase produced detailed requirements that do not reflect the internal or external realities the organization faces. |
| Development | Customers | The customers of the development phase include the business function that will operate the new work system, the IT group that will produce or configure the hardware and software, and the entire team of people who will work in the implementation phase.<br><br><u>RISKS:</u><br><br>• Business function customers inadequately involved in specifying detailed requirements.<br>• Business function customers uninvolved in testing and verifying that the software and hardware can be implemented in the organization. |
| Development | Environment | Organizational, cultural, competitive, technical, and regulatory environment within which the development phase will occur and within which the new or modified work system will be implemented.<br><br><u>RISKS:</u><br><br>• The development process ignores environmental changes that should have effected the requirements<br>• These environment-related risks apply for all phases of a project:<br>- Lack of management commitment<br>- Management unwillingness to allocate necessary resources<br>- Lack of consensus on the need for the project<br>- Lack of consensus about project governance<br>- Culture of ineffective cooperation on projects |
| Development | Infrastructure | Human, informational, and technical resources that the development phase relies upon.<br><br><u>RISKS:</u><br><br>• Development carried out based on unwarranted assumptions about the infrastructure that will support the system being produced.<br>• Development phase delayed or otherwise affected by inadequate hardware, system development software, and support. |
| Development | Strategies | The rationale under which the development phase is performed, plus the strategy of the business function, IT group, and entire firm. |

| | | |
|---|---|---|
| | | RISKS:<br><br>• The strategy of the development process is mismatched to the situation. (e.g., should have done a prototype or should have purchased more of the software) |

Table A2-4: Risks during the Implementation Phase for Any Work System

| | | |
|---|---|---|
| Implementation | Work Practices | The implementation phase includes:<br><br>• Determining the implementation approach and plan (pilot? phased? big bang?)<br>• Change management efforts about rationale and positive or negative impacts of changes<br>• Training on details of the new or revised information system and work system<br>• Conversion to the new or revised information system and work system<br>• Acceptance testing<br><br>RISKS:<br><br>• Inappropriate implementation approach is selected.<br>• Training materials and training sessions are inadequate and cause disillusionment and other problems.<br>• Training happens too early and many work system participants forget the training by the time the conversion takes place.<br>• Backup procedures prove inadequate when the initial attempt to convert encounters problems.<br>• The implementation process encounters unexpected resistance.<br>• The implementation process quashes or ignores resistance that should have provided useful feedback.<br>• The implementation involves excessive amounts of time, effort, and pain.<br>• Efforts at change management are inadequate or inappropriate |
| Implementation | Participants | Participants include all participants in the work system that is being changed plus other participants who support the implementation, such as change consultants, trainers, managers, and IT specialists.<br><br>RISKS:<br><br>• Work system participants have difficulty switching to a new way to do their work.<br>• System implementers lack interpersonal skills, empathy, and abilities related to change management.<br>• Work system participants resist the change to the new system<br>• Lack of incentives for work system participants to improve their work practices<br>• Fear that the new work system changes will lead to staff reductions and de-skilling |
| Implementation | Information | Information in the implementation phase includes specifications and training material related to the new work system, project plans, and the information that emerges during the implementation concerning progress, resistance or acceptance, and likely effectiveness of the system changes.<br><br>RISKS:<br><br>• New facts emerge during implementation showing that the new system will not be effective or will fail totally.<br>• Inadequate attention to resistance and other signals warning that the implementation is in trouble. |

| | | |
|---|---|---|
| | | • Unrealistic expectations about what work system changes are supposed to accomplish |
| Implementation | Technologies | The technologies used during the implementation phase.<br><br><u>RISKS:</u><br><br>• Bugs or non-fit related to hardware and/or software emerges during the implementation. |
| Implementation | Products & Services | The deliverables and other results produced by the implementation phase.<br><br><u>RISKS:</u><br><br>• The desired work system and/or information system is never fully implemented |
| Implementation | Customers | Customers of the implementation phase include the work system participants whose work practices are affected, managers and others responsible for work system and project results, and IT specialists who will have to maintain software and IT systems that are implemented and that might be changed during the implementation.<br><br><u>RISKS:</u><br><br>• Business managers abdicate responsibility for implementation in their organizations<br>• Work system participants (in effect, secondary customers of the implementation effort) are not well served by the methods used in the implementation or by the work system changes that are implemented. |
| Implementation | Environment | Organizational, cultural, competitive, technical, and regulatory environment within which the implementation phase will occur and within which the new or modified work system will operate.<br><br><u>RISKS:</u><br><br>• Important environmental factors change between the time when the requirements were created and the time for implementation.<br>• These environment-related risks apply for all phases of a project:<br>- Lack of management commitment<br>- Management unwillingness to allocate necessary resources<br>- Lack of consensus on the need for the project<br>- Lack of consensus about project governance<br>- Culture of ineffective cooperation on projects |
| Implementation | Infrastructure | External human, informational, and technical resources that the implementation phase will rely on.<br><br><u>RISKS:</u><br><br>• Human, technical, or informational infrastructure proves inadequate during implementation. |
| Implementation | Strategies | The rationale under which the implementation phase is performed, plus the strategy of the business function, IT group, and entire firm.<br><br><u>RISKS:</u><br><br>• The strategy of the implementation is unrealistic or otherwise flawed. (e.g., should have done a phased implementation but did a big bang implementation)<br>• The urgency in the timetable for the implementation does not match the urgency required by the surrounding strategies. |

**ABOUT THE AUTHORS**

**Steven Alter** is Professor of Information Systems at the University of San Francisco. He holds a B.S. in mathematics and Ph.D. in management science from MIT. He extended his 1975 Ph.D. thesis into one of the first books on decision support systems. After teaching at the University of Southern California he served for eight years as co-founder and Vice President of Consilium, a manufacturing software firm that went public in 1989 and was acquired by Applied Materials in 1998. His many roles at Consilium included starting departments for customer service, training, documentation, technical support, and product management. Upon returning to academia, he wrote an information systems textbook that is currently in its fourth edition, *Information Systems: Foundation of E-business*. His research for the last decade has concerned developing systems analysis concepts and methods that can be used by typical business professionals and can support communication with IT professionals. His articles appear in *Harvard Business Review, Sloan Management Review, MIS Quarterly, Interfaces, Communications of the ACM, Communications of the AIS, CIO Insight, Futures, The Futurist,* and many conference transactions.

**Susan A. Sherer** is the Kenan Professor of IT Management, Program Director of Information Systems, and co-director of the Center for Value Chain Research at Lehigh University. Sherer received her Ph.D. in Decision Sciences from the Wharton School of the University of Pennsylvania, M.S. Industrial Engineering from SUNY Buffalo, and B.S. Mathematics from SUNY Albany. Her research interests include software failure risk, managing information systems risks, inter-organizational information systems, and IT benefit justification. She is the author of *Software Failure Risk*: *Measurement and Management,* as well as articles in a variety of journals including *Information and Management, Information Systems Frontiers, Journal of Information Systems, International Journal of Electronic Commerce,* and *Communications of AIS.* Prior to moving into academia, Dr. Sherer managed projects for several manufacturing companies including Leeds & Northrup Company and Union Carbide Corporation.

Communications of the Association for Information Systems

ISSN: 1529-3181